June 3, 2013

MEMORANDUM FOR RICHARD WILLIAMS
PROGRAM MANAGER
MANAGED TRUSTED INTERNET PROTOCOL SERVICE
GSA FEDERAL ACQUISITION SERVICE

FROM: ELIZABETH F. DELNEGRO
AUTHORIZING OFFICIAL
ACQUISITION IT SERVICES

THRU: KURT D. GARBARS
SENIOR AGENCY INFORMATION SECURITY OFFICER

Subject: Security Authorization Decision:
AT&T Managed Trusted Internet Protocol Service

A security controls assessment of the AT&T Managed Trusted Internet Protocol Service (MTIPS) information system has been performed by Knowledge Consulting Group (KCG). The assessment was conducted at the FIPS 199 High Impact level in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37 R1, *Guide for Applying the Risk Management Framework to Federal Information Systems*; and the General Services Administration (GSA) Security Authorization Process.

After reviewing the results of the security controls assessment and the supporting evidence provided in the associated security authorization package, including the Security Assessment Report, System Security Plan, and Plan of Action and Milestones, together with the Penetration Test Report, Contingency Plan, and Contingency Plan Test Report, I have determined that the risk to Federal Agency operations, data, and/or assets resulting from the operation of the information system is acceptable.

Accordingly, I am issuing an Authorization to Operate (ATO) the AT&T MTIPS information system through June 3, 2016 conditioned on the following items:

1. AT&T shall resolve all open POA&M items identified during the security assessment process, per the schedule defined in the POA&M and in accordance with GSA IT Security Policy (GSA Order P. 2100.1H).

2. AT&T shall implement a process for conducting privileged authenticated vulnerability scanning no later than September 4, 2013.
3. AT&T shall provide GSA the unedited results of the vulnerability scans on a quarterly basis, in conjunction with the published GSA POA&M schedule.
4. AT&T shall resolve all items identified during the quarterly operating system, database, and web application vulnerability scans in accordance with GSA IT Security Policy (GSA Order P. 2100.1H).
5. The technical recertification activities for the next ATO shall commence no later than six months before the expiration of this ATO.

This security authorization is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system.

The security authorization of the information system will remain in effect through June 3, 2016, as long as: (i) the conditions identified above are adhered to, (ii) the required security status reports for the system are submitted to GSA; (iii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable to the GSA Authorizing Official; and (iv) the system has not exceeded the maximum allowable time period (3 years) between security authorizations in accordance with Federal or agency policy.

Copies of the authorization package are available for review at the GSA facilities in the Washington, D.C. metropolitan area. If you have any questions or comments regarding this authorization to operate, please contact Anthony Konkwo, Acquisition IT Services ISSM at 703-605-2166 or anthony.konkwo@gsa.gov.

APPROVED

X Elizabeth F. DelNegro

Elizabeth F. DelNegro
Authorizing Official

CONCURRENCE

X Kurt Garbars

Kurt D. Garbars
Senior Agency Information Security Officer